Bo-Yuan Huang

Offensive Security Research Scientist bo-yuan.huang@intel.com

Research Areas

Formal Methods | Hardware & Firmware Security | Confidential Computing | AI SoC and Graphics IPs

Education

Ph.D. in Electrical and Computer Engineering, Princeton University, 2021

M.A. in Electrical Engineering, Princeton University, 2017

B.S. in Electrical Engineering, National Taiwan University, 2014

Professional Experience

Intel Corporation, Security Research

2021–present *Offensive Security Research Scientist.* Lead formal methods research for hardware and firmware security assurance across client, data center, and AI SoCs.

- Awarded for delivering Provable Security: identified 105 security issues across 14 IPs in 7th-gen data center server SoC, achieving $190M+ cost avoidance through formal security verification.
- Awarded for leading formal firmware verification initiative: standardized and automated workflows, released open benchmark suites, and identified/fixed 9 issues in Intel TDX security service module.
- Awarded for launching company-wide Formal Imperative for pre-Si security assurance: defined negative-space and stale-data verification and drove architecture hardening of on-chip interconnect protocols.
- Awarded for managing the Intel REU program for talent-pipeline development: enabled mentorship of 70+ scholars from 30+ universities across the US.

Princeton University, Electrical and Computer Engineering

2016–2021 *Research Assistant.* Led research on Instruction-Level Abstraction for specification, verification, and design automation in heterogeneous computing systems.

Fall 2016, 17, 18 *Head Assistant Instructor.* Contemporary Logic Design; received Best AI Award.

2015–2020 *Francis Robbins Upton Fellow.*

Microsoft Research, RiSE & New Security Ventures

Summer 2019 *Research Intern.* Grammar-based fuzzing with dynamic learning for stateful REST API cloud services (US patent: 11321219 B2).

Summer 2018 *Research Intern.* White-box fuzzing for attacker-memory-safety of OS kernels with kernel-aware symbolic memory checkers on SAGE.

Intel Corporation, Security Center of Excellence

Summer 2017 *Security Research Intern.* Formal modeling and verification for concurrent firmware; exploited TOCTOU vulnerability in an inter-IPs communication protocol.

Summer 2016 *Technical Intern.* Word-level bounded model checking for Secure Boot firmware and automatic synthesis of IA semantics in QEMU.

National Taiwan University, Electrical Engineering

2013 – 2014 *Research Assistant.* Asynchronous quasi-delay-insensitive circuit synthesis.

2012 – 2013 *Research Assistant.* Game-theoretic resource allocation protocols for LTE device-to-device communications.

TSMC, Advanced Process Transferring Group

Summer 2013 *Software Engineering Intern.* Developed GDS and design pattern analysis tools.

Professional Services

Program Committee

International Conference on Automated Software Engineering (ASE): 2026 (Co-Chair)

International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS): 2023

International Conference on Computer Aided Verification (CAV): 2020

Formal Methods in Computer-Aided Design (FMCAD): 2023, 2024, 2025

International Conference on Computer-Aided Design (ICCAD): 2023, 2024, 2025

International Symposium of Electronics Design Automation (ISEDA): 2026

Patents and Publications

Patents

“Intelligently fuzzing data to exercise a service.” Patrice Godefroid, Bo-Yuan Huang, and Marina Polishchuk. In US Patent 11321219 B2, 2022.

Refereed Journal and Conference Papers

“Formal Firmware Verification of an At-Scale VM-level TEE Architecture.” Sophia Zhang, Bo-Yuan Huang, Sayak Ray, Jason Fung, Aarti Gupta, and Sharad Malik. In HOST, 2026.

“A Case Study in Firmware Verification: Applying Formal Methods to Intel TDX Module.” Dirk Beyer, Po-Chun Chien, Bo-Yuan Huang, Nian-Ze Lee, and Thomas Lemberger. In TACAS, 2026. ***Distinguished Paper Award***

“Application-Level Validation of Accelerator Designs Using a Formal Software/Hardware Interface.” Bo-Yuan Huang, Steven Lyubomirsky, Yi Li, Mike He, Gus Henry Smith, Thierry Tambe, Akash Gaonkar, Vishal Canumalla, Andrew Cheung, Gu-Yeon Wei, Aarti Gupta, Zachary Tatlock, and Sharad Malik. In TODAES, 2024.

“Generalizing the ISA to the ILA: A Software/Hardware Interface for Accelerator-rich Platforms.” Bo-Yuan Huang, Hongce Zhang, Aarti Gupta, and Sharad Malik. In DAC, 2023.

“Generating Architecture Level Abstractions from RTL Designs for Processors and Accelerators. Part I: Determining Architectural State Variables.” Yu Zeng, Bo-Yuan Huang, Hongce Zhang, Aarti Gupta, and Sharad Malik. In ICCAD, 2021.

“From DSLs to Accelerator-Rich Platform Implementations: Addressing the Mapping Gap.” Bo-Yuan Huang, Steven Lyubomirsky, Thierry Tambe, Yi Li, Mike He, Gus Smith, Gu-Yeon Wei, Aarti Gupta, Sharad Malik, Zachary Tatlock. In LATTE, 2021.

“Hardware-Software Interface Specification for Verification in Accelerator Rich Platforms.” Hongce Zhang, Bo-Yuan Huang, Yue Xing, Aarti Gupta, Sharad Malik. In LATTE, 2021.

“Intelligent REST API Data Fuzzing.” Patrice Godefroid, Bo-Yuan Huang, and Marina Polishchuk. In FSE, 2020.

“Instruction-Level Abstraction (ILA): A Uniform Specification for System-on-Chip (SoC) Verification.” Bo-Yuan Huang, Hongce Zhang, Pramod Subramanyan, Yakir Vizel, Aarti Gupta, and Sharad Malik. In TODAES, 2019. ***Best Paper Award***

“ILAng: A Modeling and Verification Platform for SoCs using Instruction-Level Abstractions.” Bo-Yuan Huang, Hongce Zhang, Aarti Gupta, and Sharad Malik. In TACAS, 2019.

“A Formal Instruction-Level GPU Model for Scalable Verification.” Yue Xing, Bo-Yuan Huang, Aarti Gupta, and Sharad Malik. In ICCAD, 2018.

“Formal Security Verification of Concurrent Firmware in SoCs using Instruction-Level Abstraction for Hardware.” Bo-Yuan Huang, Sayak Ray, Aarti Gupta, Jason Fung, and Sharad Malik. In DAC, 2018.

“Template-based Parameterized Synthesis of Uniform Instruction-Level Abstractions for SoC Verification.” Pramod Subramanyan, Bo-Yuan Huang, Yakir Vizel, Aarti Gupta, and Sharad Malik. In TCAD, 2018.

“Protocol Design and Game Theoretic Solutions for Device-to-Device Radio Resource Allocation.” Shih-Tang Su, Bo-Yuan Huang, Chih-Yu Wang, Che-Wei Teh, and Hung-Yu Wei. In TVT, 2017.

“Instruction-Level Abstraction (ILA): Democratizing Instructions for SoCs.” Bo-Yuan Huang, Hongce Zhang, Pramod Subramanyan, Yakir Vizel, Aarti Gupta, and Sharad Malik. In TECHCON, 2017. ***Best in Session Award***

“Asynchronous QDI Circuit Synthesis from Signal Transition Protocols.” Bo-Yuan Huang, Yi-Hsiang Lai, and Jie-Hong Roland Jiang. In ICCAD, 2015.

“Resource Allocation in D2D Communication—A Game Theoretic Approach.” Bo-Yuan Huang, Shih-Tang Su, Chih-Yu Wang, Che-Wei Teh, and Hung-Yu Wei. In ICC-M2M, 2014.

Others

“Early Exposure, Lasting Impact: Intel Research Program for the Next Generation of Security Leaders.” Bo-Yuan Huang. In INT31, 2025.

“A Formal Approach to Prove SAI Immutability.” Hareesh Khattri, Siva Prasad Kota, Chaturvedi Purushotam Kumar, Bo-Yuan Huang. In DTTC, 2024.

“Formal Security Verification of Root-of-Trust Firmware.” Bo-Yuan Huang, Sayak Ray, Nagaraju Kodalapura, and Jason Fung. In FVS, 2023.

“Effectiveness of Artificial Intelligence in Detecting Hardware Security Issues: Challenges, Status Quo, and Directions.” Priyam Biswas, Sayak Ray, Stephan Heuser, Bo-Yuan Huang, Rana Elnaggar, and Jason Fung. In SWPC, 2022.

Talks and Presentations

Invited Talks and Panels

“Hardening Security of HW IPs by Verifying Their Negative Space Formally.” Jasper User Group, 2025.

“Navigating the Job Search in Industry and Beyond.” Ivy Collective, 2024.

“Back to the Future: Scopes and Opportunities of AI in Hardware Security.” DTTC, 2022.

“Instruction-Level Abstraction & ILAng: A Modeling and Verification Platform for SoCs.” University of Washington, 2021.

“Instruction-Level Abstraction for Accelerator-rich Architectures’ Specification and Verification.” National Taiwan University, 2021.

“Instruction-Level Abstraction for Software Development and Verification in Accelerator-rich Computing Systems.” Intel Labs, 2021.

Tutorials

“Formal Information Flow Verification for Hardware CWEs.” DTTC, 2022.

“Generalizing the ISA to the ILA: A Software/Hardware Interface for Accelerator-rich Platforms.” ISCA, 2022.

“Generalizing the ISA to the ILA: A Software/Hardware Interface for Accelerator-rich Platforms.” ADA Center Annual Symposium, 2022.

Awards and Honors

2026	ETAPS Distinguished Paper Award
2023, 2025	Security Center of Excellence Divisional Award, Intel
2022–2025	Product Assurance and Security Divisional Award, Intel
2022	Corporate Quality Award, Intel
2020	ACM TODAES Best Paper Award
2019	Best Assistant Instructor Award, Princeton University
2017, 2018	NSF SSFT Full Scholarship
2017	SRC TECHCON Best in Session Award
2016	NSF VMW Full Scholarship
2015	Francis Robbins Upton Fellowship, Princeton University
2014	First Prize: Outstanding Undergraduate Independent Research, NTU
2014	Second Prize: TSMC Special Research Competition
2012	First Prize: TSMC Semiconductor Elite Program
2012	First Prize: Microsoft WP Platform Workshop Innovation Award
2011–2014	President’s Awards, NTU

This curriculum vitae was last updated on 6th February, 2026.